IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

COURTHOUSE NEWS SERVICE, Plaintiff, v. JACQUELINE C. SMITH, in her official capacity as Clerk of the Circuit Court for Prince William County, Virginia, Defendant, and THE COMMONWEALTH OF VIRGINIA, Intervenor-Defendant.	Civil Action No. 3:21-cv-00460-HEH

DEFENDANT COMMONWEALTH OF VIRGINIA'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT

The Commonwealth of Virginia (the "Commonwealth"), by counsel, hereby submits its memorandum of law in support of its motion for summary judgment. It states the following:

INTRODUCTION

Plaintiff Courthouse News Service ("Plaintiff" or "CNS") challenges the constitutionality of Virginia's statutory scheme governing remote access to court records. Each Virginia circuit court clerk maintains civil court records, which the public may access by visiting the courthouse. In addition to this public access, some Virginia circuit court clerks also permit Virginia-licensed attorneys, their agents, and certain governmental agencies to view nonconfidential court records online through a paid-subscription system called Officer of the Court Remote Access ("OCRA").

CNS's lawsuit is premised on the notion that if Virginia's judicial system offers licensed attorneys remote access to civil court records via paid subscriptions, then the First Amendment compels it to also offer that same access to everyone. ECF No. 21 ¶ 76; ECF 48 at 9.

The Constitution, however, does not mandate online public access to records. Instead, the reasonable statutory restrictions on online court record access are narrowly tailored to further significant governmental interests. Limiting online access to court records—many of which contain private and personally identifiable information—to a narrow class of qualified court officers promotes critical privacy and security interests by sharply reducing the amount of private, sensitive information let out into the world, limiting the potential for widespread information harvesting, resale, and dissemination. Unlike reporters or the general public, licensed attorneys are subject to professional ethical rules that further reduce the risk that private information in court records will be misused. The "time and expense" required to review "documents in person," ECF No. 21 ¶ 77, similarly minimizes privacy risks through "practical obscurity". In the language of privacy scholars, information contained in court files stored at courthouses is "practically obscure" due to the logistical barriers to amassing large amounts of private information. Due to those barriers, private and sensitive information can appear in public records without creating a risk of actual widespread public disclosure or harm. David S. Ardia, *Privacy and Court Records: Online Access and the Loss of Practical Obscurity*, 2017 U. Ill. L. Rev. 1385 (2017).

Of course, the press and public enjoy a qualified right of access to nonconfidential civil court records, which helps ensure the transparency of the courts. But that right of access is qualified because it must not undermine the fair, orderly, and efficient administration of government. Unlimited public OCRA access would allow third parties interested in obtaining

private information to write a computer script and download every social security number ever printed on the face of a court record in a jurisdiction, exposing vulnerable litigants to harmful data mining and exploitation— all from anywhere in the world. The Constitution does not require Virginia's judicial system to facilitate such exploitation. Accordingly, this Court should grant the Commonwealth's motion for summary judgment.

FACTS

The parties' Joint Stipulations of Fact, Dkt. No. 55, provide the relevant facts supporting the Commonwealth's Motion for Summary Judgment. In addition to these stipulations, the Commonwealth has identified further undisputed facts supporting its substantial governmental interests in protecting the private information contained in nonconfidential court filings while preserving the fair, orderly and efficient administration of justice. *See Courthouse News Serv. v. Schaefer*, 2 F.4th 318, 328 (4th Cir. 2021). These additional facts demonstrate that OCRA would be particularly vulnerable to malicious and exploitative data mining if it were available to the public at large.

Data capture and analysis is an emerging and highly lucrative field of business in the modern world. There are innumerable ways in which entities harness data for commercial use. For instance, Major League Baseball records 24 terabytes of video per game to be analyzed by a team's analytics department;[1] musicians take data gleaned from virtual concerts to tailor their shows to future audiences;[2] satellites, aircraft, and ocean buoys provide data to scientists who can measure climate change via temperatures, ocean currents, soil moisture, air quality, cloud

[1] Paul Overberg & Kevin Hand, *How to Understand the Data Explosion*, Wall St. J. (Dec. 8, 2021, 11:00 AM), https://tinyurl.com/mr2efah5.
[2] Anne Steele, *Armed With Data, Musicians Have Big Plans to Court Their Superfans*, Wall St. J. (Dec. 7, 2021, 10:00 AM), https://tinyurl.com/mwap8r9s.

cover, and hundreds of other phenomena on Earth and in its atmosphere.[3]

Mass data harvesting, however, can also be used for criminal and quasi-criminal purposes. Personally Identifiable Information ("PII"), such as social security numbers, original signatures, and bank account numbers can be harvested from records to uniquely identify and even impersonate an individual. Bad actors can use an identification based on harvested PII to wreak financial havoc. With small amounts of PII, thieves can, for example, "create false accounts in the person's name, incur debt, create a falsified passport or sell a person's identity to a criminal."[4] As a result, a host of federal and state laws regulate the collection, use, processing, and disclosure of PII, including, for example, the Federal Trade Commission Act. 15 U.S.C. §§ 41-58; *see, e.g.*, *In re: Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374 (E.D. Va. 2020) (discussing Section 5 of the FTC Act creating enforceable duties with regards to data breaches); *see also* Va. Code § 59.1-442 *et seq.* (creating a right of action for individuals aggrieved by the improper use of purchaser information, dates of birth, social security numbers, or driver's license information).

Beyond the potential for identify theft and other criminal exploitation, there is growing concern that mass data harvesting—even data from the legal sale of aggregated, publicly available information—can be a threat to democracy.[5] The concerns related to legal uses of data harvested from public records were raised as early as 2013 in a government report to the chairman of the Senate Committee on Commerce, Science, and Transportation.[6] The Data

---

[3] Robert Lee Hotz, *Climate Change Data Deluge Has Scientists Scrambling for Solutions*, (Dec. 5, 2021, 11:00 AM), https://tinyurl.com/mtscjps6.
[4] Corinne Bernstein, *Personally Identifiable Information*, TechTarget, https://tinyurl.com/yms4p8um (last visited July 6, 2022).
[5] *See, e.g.*, John Sherman, *Data Brokers Are a Threat to Democracy*, Wired (Apr. 13, 2021), https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/.
[6] Office of Oversight and Investigations Majority Staff. "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes," Staff Report for Chairman

Broker Report noted that publicly available "government records" were a major source of consumer data sold by data brokers.[7] Data brokers mined "court filings, including criminal convictions, judgments, liens, and bankruptcies"[8] for data to resell.[9] The brokers willingly purchased access to databases containing personal information.[10] The Data Broker Report observed that although "the practice of collecting and selling consumer data . . . has existed for many decades," by 2013, "[i]nformation that was previously public but required a trip to places such as a library or courthouse to retrieve can now be instantaneously accessible to millions when posted on the Internet."[11] Data brokers sort, aggregate, and analyze this now-easily accessible information to a wide variety of buyers who use it for purposes including marketing, for determining if a person is a good risk for employment, insurance, or credit, or even to target "financially vulnerable customers" who are likely to take out payday loans and other exploitative financial products.[12] In short, mass data mining of easily accessible public records can be used for criminal ends, and even when information is not used to commit a crime, it can be used to identify and target vulnerable individuals for exploitation.

Virginia's publicly available court databases are not immune from data mining, as the

---

Rockefeller, Dec. 18, 2013, https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a (last visited July 5, 2022). [hereinafter "Data Broker Report"]. Courts may take judicial notice of public records. *Philips v. Pitt Cnty. Memorial Hosp.*, 572 F3d 176, 180 (4th Cir. 2009). Reports to Senate Committees are public records. *See* S.C. v. United States, 2017 U.S. Dist. LEXIS 35946 (D. S.C. 2017) (citing to records provided to government sources or generated by government sources and available either online or by request as being "public records" that can be considered even at the motion to dismiss stage).

[7] Data Broker Reporter at 15.

[8] Privacy scholars have noted that data brokers such as Acxiom, ChoicePoint, and LexisNexis routinely mine court records for PII, specifically. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. rev. 435, 457 (2008).

[9] Id.

[10] Id.

[11] *Id.* at 1-2.

[12] *Id.* at "Executive Summary."

Office of the Executive Secretary of the Supreme Court of Virginia ("OES")—the entity that supplies all information technology and technical support to the courts in the Commonwealth[13]—has discovered. **Declaration of Joby Knuth, attached as Exhibit A**. In creating technology solutions and in providing technical support, OES must comply with Virginia's laws governing the use of technology as applied to court records and the public policy concerns that animate those statutory restrictions. Va. Code § 2.2-2009(A) (providing that the Chief Information Officer of the Virginia Information Technologies Agency shall develop policies, standards, and guidelines for assessing and mitigating unauthorized data usage that "shall apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies."); *see also* Dkt. No. 55 ¶¶ 33-34 (VITA's Security Standard for Restricted Remote Access to Documents on Court-Controlled Websites).

OES applies these security standards in its development and maintenance of a variety of applications for usage by the courts. *See* Dkt. No. 55 ¶¶ 29-31; **Exhibit B** ¶ 2. These applications include the Circuit Court Case Management System ("CCMS"), the Case Imaging System ("CIS"), and OCRA, an application developed by OES for circuit courts that used CIS. Dkt No. 55 ¶ 35. OES also develops and maintains applications for public use, including the General District Court Online Case Information System ("General OCIS"), the Circuit Court Online Case Information System ("Circuit OCIS"), Online Case Information System 2.0 (OCIS 2.0), and the Virginia Date of Birth Confirmation ("VDBC"). **Exhibit A** ¶ 3. Circuit OCIS allows users to search for court cases in specific, participating circuit courts, using party name, case number, or hearing date.[14] Responsive results will show case numbers, party names, date and time of the

[13] *Office of the Executive Secretary*, Virginia's Judicial System, https://www.vacourts.gov/courtadmin/aoc/oes/home.html (last visited July 7, 2022).
[14] *See* Circuit OCIS, ewsocis1.courts.state.va.us/CIJSWeb/Main Menu.do (last visited July 8, 2022).

next hearing, the hearing type, and the result of the case.[15] For civil cases, selecting a result will identify the attorneys, all hearings, whether judgment has been entered, the date of the final order, a list of pleadings and orders (without showing the filed documents), and whether or not service was effectuated.[16] For criminal cases, Circuit OCIS shows similar information, along with charging information and the defendant's race, sex, date of birth (with the year redacted), and ZIP code. General OCIS provides nearly identical information in response to search queries.[17]

Despite adherence to VITA's security standards, both of these systems have been subject to data harvesting tactics. **Exhibit A** ¶ 8. In 2010, for example, Joby Knuth—the Deputy Director – Application Development Manager for OES—found an inordinate amount of traffic coming from IP addresses identified as "bots"[18] through log analysis.

> Our algorithms identified sessions in which search activities resembled those typically associated with non-human behavior. For example, instead of searching for a few cases or names within a single session, the bots would enter searches for every single possible case number within the database, sequentially. They would additionally make requests, per second, far faster than what a human is capable of entering.

Id. ¶ 9.

The VDBC is another system designed by OES "for individuals within a registered organization to confirm a consenting individual's last name, date of birth, and last four digits of

---

[15] Id.
[16] Id.
[17] *Id.*

[18] A "bot" is a computer program that operates as an agent for a user or other program. Bots are used to automate tasks and therefore can operate without specific input from a human user once activated. Bots can replace a repetitive task a human would otherwise have to perform and are often faster at performing those tasks than a human user would be. One common task for a bot program is to gather information from websites. Ben Lutkevich & Alexander Gillis, *Definition: Bot*, TechTarget, https://www.techtarget.com/whatis/definition/bot-robot (last visited Jul. 6, 2022).

the social security number associated with criminal and traffic cases maintained in the general district court case management system." *Id.* ¶ 11. Using the VDBC, a user searches based upon any combination of the following: a full last name, partial first name, full date of birth, the last four digits of a security number, a driver's license number and/or the driver's license state. *Id.* ¶ 12. The system searches the cases available on Circuit OCIS and General OCIS and returns a list of cases which match the entered information. *Id.* It additionally gives a column for whether the entered terms match those in the results. *Id.* The VDBC does not show PII, but one can glean PII by coding an algorithm with partial PII and determine by process of elimination. *Id.*

By its registrant agreement, the VDBC specifically prohibits data harvesting practices. *Id.* ¶ 13. Despite the registrant agreement, the VDBC has been, and continues to be, subjected to data harvesting tactics by bots. *Id.* ¶ 14. Mr. Knuth has observed bots searching for PII using very fast searching, entering searches using the last name and partial information to confirm social security numbers. *Id.* Although the social security numbers are not shown, when a hit is shown in response to a search, the "guessed" information on the search confirms the PII. *Id.* Mr. Knuth has expressed that anti-scripting tactics deployed to counter bot activity have had limited success. *Id.* ¶ 16. Because bots can quickly determine how their activity is being detected, bots will adapt their algorithms to avoid detection. *Id.* The bots can continue to collect data in violation of the registration terms, albeit usually more slowly, but nevertheless usually slip past detection. *Id.* And upon receiving a ban, a determined harvester can simply reapply for access to the VDBC using a different IP address. *Id.* While the VDBC utilizes a registrant agreement, there is no real way to vet registrants because the system is open for use to the general public. *Id.* As a result, the VDBC continues to be mined for data. *Id.*

Unlike the VDBC which links to aggregated data pulled from online case information, OCRA provides digital copies of actual court records. Dkt. No. 55 ¶ 35; Va. Code § 17.1-293(E)(7). These records contain unredacted PII because the Code of Virginia permits clerks to post PII online if it is posted to OCRA. *Id.* In addition, a clerk can choose to make Criminal, Civil, Chancery, Miscellaneous records, or any combination of these. **Exhibit B** ¶ 7. Once a clerk has determined the scope of the clerk's records that will be made available through the OCRA application, the subscriber has access to the entirety of the records made available through the OCRA application. *Id.* These records are downloadable as PDFs in OCRA. **Exhibit B** ¶¶ 4-5. This makes OCRA particularly vulnerable to data mining because there are many freely available programs which can scan through PDFs and turn the documents into searchable text and databases. **Exhibit A** ¶ 7. Persons with basic programming knowledge can develop algorithms to comb those databases for PII. This sort of data mining is impossible at courthouses where a user must print each court record at a per-page cost. *Id.*; Dkt. No. 55 ¶ 50. There is no per-page cost to access or download records through OCRA. *See* **Exhibit B** ¶ 5. Instead, users pay a one-time annual subscription fee for unlimited access to the available records. Dkt. No. 55 ¶ 43. As a result, if OCRA were to become publicly accessible, substantially more sensitive personal information would be subject to data mining and potential exploitation—a significant harm that OCRA's current limitations are narrowly tailored to prevent.

STANDARD OF REVIEW

A court should grant summary judgment "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). "As to materiality . . . [o]nly disputes over facts that might affect the outcome of the suit under the governing law will properly preclude the entry of summary judgment." *Anderson v. Liberty*

Lobby, Inc., 477 U.S. 242, 248 (1986). In order to preclude summary judgment, the dispute about a material fact must be "'genuine,' that is, if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* However, if the evidence of a genuine issue of material fact "is merely colorable or is not significantly probative, summary judgment may be granted." *Id.* at 250. In considering a motion for summary judgment under Rule 56, a court must view the record as a whole and draw all reasonable inferences in the light most favorable to the nonmoving party. *See, e.g., Celotex Corp. v. Catrett*, 477 U.S. 317, 322-24 (1986).

Where a nonmoving party fails to establish an essential element of his case, all other facts are rendered immaterial, and entry of summary judgment is required as a matter of law. *Celotex Corp.*, 477 U.S. at 322-23. The purpose of summary judgment is to facilitate the "prompt disposition of controversies on their merits without a[n] [unnecessary] trial, if in essence there is no real dispute as to the salient facts." *Bland v. Norfolk & Southern RR Co.*, 406 F.2d 863, 866 (4th Cir. 1969). When a careful consideration of the record reveals the absence of any genuine issue of material fact, it is "the affirmative obligation of the trial judge to prevent 'factually unsupported claims and defenses' from proceeding to trial." *Felty v. Graves-Humphreys Co.*, 818 F.2d 1126, 1128 (4th Cir. 1987) (citation omitted).

ARGUMENT

Given the sensitivity of the information available on OCRA and its susceptibility to malicious data mining, the General Assembly has provided that only licensed Virginia attorneys, their authorized agents, and certain governmental entities may access OCRA. Va. Code § 17.1-293(E)(7). To further protect against abuses, the legislature has also prohibited OCRA users from publicly disseminating the data obtained from OCRA access. Va. Code § 17.1-293(H). Where a limitation on a right of access resembles a "time, place, and manner" restriction, the

Court applies relaxed scrutiny. Dkt. No. 48 at 10 (citing *Globe Newspaper v. Superior Ct. for Norfolk Cty.*, 457 U.S. 596, 607 n. 17 (1982)). As this Court has previously observed, "[t]he non-attorney access restriction challenged here does not stop CNS from accessing civil court records altogether but instead controls how and when it accesses them. Thus, it resembles a time, place, and manner restriction and relaxed scrutiny applies." *Id.* "In this case, relaxed scrutiny requires the limitation to be content-neutral, narrowly tailored and necessary to preserve a significant governmental interest." *Id.* (citations and internal quotations omitted). Because the statutory limitations on OCRA access and dissemination are narrowly tailored to further significant government interests, they do not violate the First Amendment. As such, this Court should grant summary judgment for the Commonwealth.

I. OCRA's non-attorney access and dissemination limitations are content neutral because they do not turn upon the communicative content of the court records.

The non-attorney access and dissemination limitations apply to all non-confidential filings equally; therefore, the limitations are content-neutral. "To be content-neutral, the [challenged] policy cannot target speech based on its communicative content, or draw distinctions based on the message a speaker conveys." *Courthouse News Serv. v. Planet*, 947 F.3d 581, 601 (9th Cir. 2020) (citing *Reed v. Town of Gilbert*, 576 U.S. 155 (2015) (internal quotations omitted). "A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others." *Ward v. Rock Against Racism*, 419 U.S. 781, 791 (1989).

The non-attorney access limitation does not change based on viewpoint or subject matter, nor does it discriminate among classes of the public seeking access to records, instead limiting it to attorneys, who have ethical obligations as court officers. No facts revealed in discovery have

shown that Clerk Smith discriminates among media outlets in granting or denying access to OCRA, nor has CNS pleaded that Clerk Smith does. In addition, the access and dissemination limitations apply equally to all court records in the system, and do not turn upon the communicative contents of the court records. Va. Code § 17.1-293; *see* Dkt. No. 55 ¶ 27 (stating that the Prince William Clerk provides to all subscribers "remote online access to electronic images of *all* non-confidential civil court records filed within the Prince William Circuit Court . . .")' Accordingly, the access and dissemination limitations are content neutral.

Although not advanced by CNS as this stage in the litigation, it is important to note that because the First Amendment would prohibit granting or denying access based on viewpoint, there is no meaningful way for clerks or the Commonwealth to craft a rule or law limiting access to members of the press. *See* Transcript of Motions to Dismiss and Initial Pretrial Conference, Dkt. No. 46 at 26 (suggesting that a legislative remedy would address CNS's claims). CNS is likely to claim, just as it did at the Motion to Dismiss stage, that as journalists, its employees are bound by a set of ethical standards, just as attorneys are. *Id.* at 37. But the First Amendment applies to even self-styled "citizen journalists" who publish their content on social media outlets, instead of through a traditional news outlet. *Lovell v. City of Griffin*, 303 U.S. 444, 452 (1938) ("The liberty of the press is not confined to newspapers and periodicals. . . . The press in his historic connotation comprehends every sort of publication which affords a vehicle of information and opinion."). Simply put, "a reporter's constitutional rights are no greater than those of any member of the public." *Estes v. Texas*, 381 U.S. 532, 589 (1965) (Harlan, J., concurring).

Therefore, there is no meaningful way to limit OCRA access to members of the press without risking viewpoint discrimination by only sanctioning accounts for journalists writing for

"mainstream" media news sources. In today's world, anyone who can create a Facebook, Twitter, TikTok, or Instagram account has access to a publishing medium that is "a vehicle of information and opinion" and can therefore claim they are journalists entitled to the same access as CNS. *Id.* Thus limiting access to Virginia Bar licensed attorneys, but excluding even members of the press is narrowly tailored to serve the state interest in protecting the privacy of the information.

II. OCRA's non-attorney access and dissemination limitations further the Commonwealth's interest in the fair and orderly administration of justice by limiting the widespread dissemination of litigants' PII.

The fair and orderly administration of justice is a significant interest for the Commonwealth of Virginia and its courts. *Courthouse News Serv. v. Schaefer*, 2 F.4th 318, 328 (4th Cir. 2021). The Commonwealth promotes the fair and orderly administration of justice in promoting the privacy rights of its litigants, such that they will not be disincentivized from seeking out the justice system to vindicate their rights. *See Courthouse News Serv. v. Planet*, 947 F.3d 581, 604 (9th Cir. 2020). The Supreme Court has repeatedly held that protecting citizen privacy, particularly within the justice system, is a significant government interest. *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 596 (2011) ("[T]his Court has affirmed the importance of maintaining "privacy" as an important public policy goal—even in respect to information already disclosed to the public for particular purposes (but not others).") (citing *Dept. of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 762-771 (1989)); *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 34-35, n. 22 (1984) (acknowledging the government's significant interest in protecting the privacy interests of litigants and third parties in civil litigation and finding that a protective order prohibiting a newspaper from publishing information which it had obtained through discovery procedures did not offend the First Amendment).

OCRA's access and dissemination limitations further the Commonwealth's significant interest in preventing widespread disclosure of the private information of litigants. Virginia Code § 17.1-293(B) prohibits a clerk from posting highly sensitive, private information online. This information includes actual signatures, dates of birth identified with a particular person, the maiden name of a person's parent so as to be identified with a particular person, any financial account number or numbers, or the name and age of any minor child. *Id.* at (B). A clerk is also forbidden from disclosing driver's license information, information on credit cards, debit cards, and other financial information. *Id.* at A. The Code states, however, that clerks may post the information described in either (A) or (B) on OCRA. Va. Code § 17.1-293(E)(7).

Virginia Code § 8.01-420.8, which applies only to civil litigants, places redaction requirements on attorneys and litigants. This section requires redaction of "all but the last four digits of the identification number" of social security numbers, driver's license numbers, and credit card, debit card, bank account, or other numbers associated with electronic billing and payment systems. *Id.* at (A). The Code explicitly waives civil liability "against the party or lawyer who filed the document or any court personnel, the clerk, or any employees of the clerk's office who received it for filing." *Id.* at (C). Thus, the redaction requirements do not cover the entirety of the sensitive information described in Code § 17.1-293(A)-(B). Further, empirical analysis shows that PII routinely finds its way into court filings even when redaction requirements are imposed. *See generally* David S. Ardia & Anne Klinefelter, *Privacy and Court Records: An Empirical Study*, 30 Berkeley Tech. L.J. 1807, discussed *infra* at 21.

But in Virginia, the PII reflected on those records is accessible on the internet only to lawyers, a self-policing, pre-vetted group subject to codified Rules of Professional Conduct and serious professional sanctions for violating those Rules. *See* Rules of the Supreme Court of

Virginia, Part Six, § II. Thus, publishing PII on OCRA carries far fewer risks than generally broadcasting it to the entire world via the internet, and the enforcement mechanism for misuse is more than what is imposed just by the user agreement.

Public access to records at a physical courthouse serves as a bulwark against widespread dissemination of the private information contained in court records. *See Dept. of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 764 (1989).[19] If, however, the Court finds that OCRA's attorney-only limitation is unconstitutional and eliminates it, any entity or individual from across the United States would have unfettered, unlimited access to the entirety of Virginia litigants' private information. Without these protective time and cost burdens, any entity could write an algorithm to harvest private information from each circuit court's filings, using that information to the detriment of Virginia litigants. *See* **Exhibit A** ¶ 7.

In contrast to members of the public, lawyers need the PII contained in court records to perform their jobs effectively. For example, attorneys practicing family law need access to pleadings reflecting the names and ages of minor children. Attorneys litigating a civil fraud case might need copies of pleadings reflecting the actual signatures of the parties or witnesses. Attorneys practicing collections work need access to financial information in order to identify assets and satisfy judgments. The instances where attorneys would need such private information to do their jobs are numerous; the instances where the public at large would need such information are not. Further, the efficiency of the justice system depends on attorneys gaining

[19] In *Reporters Committee*, the United States Supreme Court anticipated this exact problem, and specifically noted "the vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations through the country and a computerized summary located in a single clearinghouse of information." *Id.* at 764. The Court additionally noted "the fact that an event is not wholly private does not mean that an individual has no interest in limiting disclosure or dissemination of the information." *Id.* at 770.

access to this information remotely – attorneys cannot waste days traveling from jurisdiction to jurisdiction to get hard copies of these filings, which may or may not be relevant for their purposes. Time spent traveling to and from courthouses is time that better spent performing any number of advocacy-related activities. It is also time that the attorney will not have to bill to a client, which makes affording competent representation in court matters more cost effective, lowering the barriers to justice for those who have fewer assets to satisfy legal fees.

The Commonwealth balances its promotion of effective advocacy with the need for protecting litigants' private information by generally restricting clerks from posting PII online except on OCRA. Va. Code § 17.1-293(E)(7). Limiting access to this potentially exploitable "clearinghouse of information", *Reporters Comm. for Freedom of Press*, 489 U.S. at 764, to Virginia-licensed attorneys is secured by the fact that lawyers are self-policing. As members of the Virginia State Bar, lawyers self-regulate subject to the Virginia Rules of Professional Conduct (the "RPC"):

> The legal profession is largely self-governing. Although other professions also have been granted powers of self-government, the legal profession is unique in this respect because of the close relationship between the profession and the processes of government and law enforcement. This connection is manifested in the fact that the ultimate authority over the legal profession is vested largely in the courts . . . To the extent that lawyers meet the obligations of their professional calling, the occasion for government regulation is obviated.
>
> Pmbl. to the Va. R. Prof'l Cond.

Consistent with self-regulation, lawyers are held to a higher standard than the public and face losing their livelihoods should they fail to meet those standards. A Virginia-licensed attorney found in violation of the RPC faces sanctions, which can include suspension or revocation of his or her license to practice law in Virginia. *See generally* Va. Sup. Ct. R. part 6, § IV ¶ 13. And the RPC prohibit improper usage of private information obtained from either

clients or third parties. Va. Sup. Ct. R. part 6, § II, R. 1.6 (Confidentiality of Information), R. 4.4(a) (Respect for Rights of Third Persons), R. 8.4 (Misconduct)[20].

Lawyers are also less likely to abuse the system not only because they risk public censure and their livelihoods for violating the Virginia RPC, but because they have been pre-vetted by the Virginia State Bar's Character and Fitness review in a way that clerks could never do with a subscriber agreement. *See* **Exhibit A** ¶ 16. Simply put, lawyers must be trusted to protect confidences; their duty to protect these confidences promotes, in turn, the public's confidence in the justice system.

> A lawyer's responsibilities as a representative of clients, an officer of the legal system and a public citizen are usually harmonious . . . [A] lawyer can be sure that preserving client confidences ordinarily serves the public interest because people are more likely to seek legal advice, and thereby heed their legal obligations, when they know their communications will be private.
>
> Pmbl. to the Va. R. of Prof'l Cond.

The Supreme Court of the United States has additionally recognized the important role that protecting privacy plays in maintaining the integrity of the justice system:

> [As] the trial court rightly observed, rather than expose themselves to unwanted publicity, individuals may well forgo the pursuit of their just claims. The judicial system will thus have made the utilization of its remedies so onerous that the people will be reluctant or unwilling to use it, resulting in frustration of a right as valuable as that of speech itself.

Seattle Times Co. v. Rhinehart, 467 U.S. 20, 35 n. 22 (1984) (quoting *Rhinehart v. Seattle Times Co.*, 98 Wash. 2d 226, 254 (1982)).

The *Rhinehart* Court's reasoning applies with equal force here—the Commonwealth protects the widespread dissemination of litigants' PII by limiting OCRA access to attorneys. If

[20] Rule 8.4(b) specifically prohibits conduct, either criminal or "deliberately wrongful", which implicates a "serious interference with the administration of justice." Va. Sup. Ct. R. part 6, § II, R. 8.4(b), cmt 2.

the Commonwealth did not limit OCRA access to attorneys, but instead broadcast litigants' PII across the world, litigants would be disincentivized from vindicating their rights in court,[21] directly undermining the Commonwealth's significant government interest in the "fair and orderly administration of justice." *Courthouse News Serv. v. Schaefer*, 2 F.4th 318, 328 (4th Cir. 2021).

Virginia's approach of refraining from posting non-confidential court records online for public consumption is consistent with the practices of all other states in the Fourth Circuit, except for South Carolina, in which some, but not all, jurisdictions within the state post court records online. Dkt. No. 55 ¶ 10. North Carolina does not grant public access to court records, but maintains civil and criminal databases, similar to Virginia's Circuit OCIS, General OCIS, and OCIS 2.0, in which North Carolina prioritizes usage by court personnel, such as judges, clerks of court, public defenders, "and other State and local government agencies that access the system in order to perform their legal duties . . ." Remote Public Access Program, North Carolina Judicial Branch, https://www.nccourts.gov/services/remote-public-access-program (last visited July 8, 2022); RPA Online Access, Sample Licensing Agreement – Online Access, tinyurl.com/2p9sz9n6. In fact, very few states provide online access to court records to all members of the public. Dkt. No. 55 ¶ 10. Some of the states that provide online access to non-confidential court records exclude entire categories of records from that remote online access, posing serious problems under the "content neutrality" prong of a time, manner, or place restriction. *See, e.g.*, Colo. Judicial Dep't, Public Access to Court Records §§ 4.20(b), 4.60.

[21] "Indeed, we are already seeing privacy concerns drive an increase in the use of alternative dispute resolution ("ADR") procedures, particularly confidential arbitrations where no public right of access exists at all. Potential litigants who cannot afford ADR may simply view the privacy costs as too great and decide not to seek resolution in the courts – or worse, engage in self-help remedies." David S. Ardia, *Privacy and Court Records: Online Access and the Loss of Practical Obscurity*, 2017 U. Ill. L. Rev. 1385, 1446-48 (2017) (citations omitted).

III. OCRA's non-attorney access and dissemination limitations are narrowly tailored because the Commonwealth would achieve its interests less effectively without them.

OCRA's access and dissemination limitations protect the privacy of its litigants, which in turn promote the fair and orderly administration of justice. Adopting any other system of remote access would render litigants' private information less secure than it is on OCRA; accordingly, the challenged restrictions are narrowly tailored.

In the context of a time, place and manner restriction, "[a] regulation is narrowly tailored . . . if it promotes a substantial government interest that would be achieved less effectively absent the regulation and does not burden substantially more speech than is necessary to further the government's legitimate interests." *Ross v. Early*, 746 F.3d, 546, 552-53 (4th Cir. 2014) (quotation omitted). "In this vein, the regulation need not be the least restrictive or least intrusive means of serving the government's significant interests." *Id.* (citation and internal quotations omitted). "So long as the means chosen are not substantially broader than necessary to achieve the government's interest, however, the regulation will not be invalid simply because a court concludes that the government's interest could be adequately served by some less-speech restrictive alternative." *Ward v. Rock Against Racism*, 491 U.S. 781, 800 (1989).

For two reasons, the Commonwealth would achieve its substantial government interests less effectively if OCRA's non-attorney access limitation were eliminated. First, if OCRA were available to the global[22] community, the Commonwealth would have to pass a host of legislation

[22] "It is long settled as a matter of American constitutional law that foreign citizens outside U.S. territory do not possess rights under the U.S. Constitution." *Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 140 S. Ct. 2082 (2020). Therefore, non-citizens residing outside the U.S. do not have a right of access to Virginia's court records, online or otherwise. Practically speaking, however, it would be difficult to limit OCRA access to only people residing in the U.S. and citizens residing abroad, without requiring either a lengthy application and some vetting of the documents provided to verify the person or company seeking access is a U.S. resident or U.S. citizen residing abroad. In addition, American data brokerage companies could sell the harvested

to protect the widespread distribution of PII, placing significant time and cost burdens on both clerks and litigants to both redact all filings or make separate filings containing PII. Empirical studies have shown redaction in particular to be an ineffective method at preventing PII and other sensitive information from appearing in non-confidential court records. Second, the Commonwealth and the clerks would be forced to expend substantial resources to aggressively police OCRA user activity to limit exploitation of personal information, likely with less success than under the current access restrictions.

a. Redaction has shown to be ineffective at preventing PII and other sensitive information from appearing in court records.

In 2018, OES convened a Working Group to examine, among other things, the legislative ramifications of eliminating OCRA's non-attorney access limitation. Dkt. No. 55 ¶ 52 (the "Work Group Report"). The group, mostly comprising circuit court clerks and legislative consultants, found that opening OCRA to the public would require drastic alterations to the Commonwealth's legislative scheme to prevent private information from being leaked to the public. Work Group Report at 13. At a minimum, opening OCRA to the public would require litigants or clerks to redact all filings, and litigants would have to provide separate filings, both redacted and unredacted. *Id.* OCRA's current attorney-only access limitation threads the needle by balancing the need for convenient, around-the-clock access at a cost to the parties who need it most: attorneys, clerks, and government agencies, while providing a measure of "practical obscurity" for the PII in court filings by making access a little more onerous but at a much lower cost for the general public.[23]

---

data abroad.

[23] Access to records at a courthouse is free via public access terminals. Dkt. No. 55 ¶ 46. Members of the public are typically only charged for the nominal cost of making a paper copy of the record. *Id.* ¶ 50.

But relying on redaction is not enough to protect PII. Even if all of the proposed legislative fixes were passed, research has shown that redaction rules have limited efficacy in preventing widespread disclosure of sensitive information. For example, in 2009 Carl Malamud used automated software to search a large sample of court filings downloaded from the federal court's Public Access to Court Electronic records (PACER) system. Malamud reported to the federal courts that a significant number of social security numbers and other types of sensitive information were present in the downloaded files. *See* Letter from Carl Malamud to The Honorable Lee H. Rosenthal, Chair, Committee on Rules of Practice and Procedure, Judicial Conference of the United States (Oct. 24, 2008), https://public.resource.org/scribd/7512583.pdf (documenting 1,669 unredacted social security numbers and other proximate sensitive information in records from 32 district courts). In addition, computer scientist Timothy Lee followed Malamud's report with a study that found some documents submitted to courts with intended redactions were not successfully redacted. Timothy B. Lee, *Studying the Frequency of Redaction Failures in PACER*, Freedom to Tinker (May 25, 2011), https://freedom-to-tinker.com/blog/ tblee/studying-frequency-redaction-failures-pacer.

Likewise, a 2015 empirical study in North Carolina showed a high frequency of sensitive information included in state court filings. David S. Ardia & Anne Klinefelter, *Privacy and Court Records: An Empirical Study*, 30 Berkeley Tech. L.J. 1807. North Carolina prohibits litigants and attorneys from filing documents which include "any person's social security, employer taxpayer identification, drivers license, state identification, passport, checking account, savings account, credit card, or debit card number, or personal identification (PIN) code or passwords in that document . . ." N.C. G.S. 132.1-10(d). This prohibition on filing sensitive information is broader than Virginia's redaction statute, Va. Code § 8.01-420.8, and even carries

a penalty of five hundred dollars ($500) for violating. *Id.*

To determine the rate at which sensitive information appeared in North Carolina filings despite these requirements, the 2015 empirical study analyzed nonconfidential briefs submitted to the North Carolina Supreme Court from 1984 to 2000. *Privacy in Court Records*, 30 Berkeley Tech L.J. at 1816. Based on a survey or privacy laws and privacy scholarship, the researchers created a taxonomy of thirteen categories of sensitive information, such as "Financial Information," "Identity," "Location," "Health," and "Sexual Activities," among others. *Id.* at 1837 *et seq.* They required that these sensitive information types be associated with individuals named within the court briefs. *Id.* at 1836 n. 101. They then coded a stratified random sample of 504 court filings "in order to determine the frequency of appearance of each sensitive information type . . ." *Id.* Of the 504 filings, 336 contained "Location" information, 331 contained "Identity" information, 175 contained information related to "Assets" and 134 contained "Financial Information." Just 37 of the documents in the sample contained no sensitive information. *Id.* at 1860, Table 4. The study also showed that information associated with criminal proceedings, such as witness and crime victim names, was pervasive in court records, appearing in civil cases as well as criminal, and that criminal filings showed a disproportionately high level of sensitive information. *Id.* at 1883-1886. Finally, the study failed to show any increase or reduction in the frequency of sensitive information included in the filings over the seventeen-year period. *Id.* at 1889.

The results of the 2015 empirical study are indisputable – even with redaction measures in place, sensitive information will continue to appear in non-confidential court records with high frequency. Research on data brokers has shown that even PACER, a system which relies on redaction and per-page fees to deter data harvesting, is nevertheless routinely mined for data.

Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435, 457 (2008). If the Commonwealth opened OCRA to the public, there is no reason to believe that legislation requiring redaction would prevent sensitive information being leaked, despite increasing costs for litigants and the courts. *See* **Sworn Declaration of Paul Ferguson, Clerk of Arlington Circuit Court, attached as Exhibit C**, ¶¶ 8, 11.

b. Policing misuse of OCRA via subscriber agreements and anti-data harvesting programming will have limited success at preventing mass dissemination of PII.

To mitigate the limited efficacy of redaction efforts, if OCRA were opened to the public, the Commonwealth and the clerks would be forced to implement security measures to limit the spread of PII. Databases developed for public usage and maintained by OES, however, have shown that the information on those databases can, and will, be subjected to data harvesting, despite OES's best efforts to mitigate those tactics. **Exhibit A**. As stated by OES's Deputy Director – Application Development Manager, at least four of its systems developed for public usage have been, and continue to be, subjected to manual and automated data mining from around the world. *Id.* ¶ 8. Notably, none of those systems reveal the sort of sensitive information contained on documents available via OCRA, such as social security numbers, maiden names, and financial account numbers. *See* Code § 17.1-293(B),(E). , If made public, OCRA will almost certainly be subject to targeted data harvesting in the same fashion that other publicly used systems developed by OES have been, particularly when data brokers were already looking to court records for data to harvest a decade ago. *See* Data Broker Reporter at 15.

Plaintiff has alleged that potential OCRA misuse could be policed through "Subscriber Agreements," *see* Dkt. No. 48 at 11, Dkt. No. 21 ¶ 44. Prior practice, however, has demonstrated that subscriber agreements are often ignored and circumvented. **Exhibit A** ¶ 13. For instance, in submitting a registrant agreement for the VDBC, the applicants agree not to "[e]xecute any form

or automated scripting against the system," "access or attempt to access the system in an excessive manner," or "misuse search criteria or conduct searches in a manner that may be construed as attempting to gather information for purposes other than that for which the system was designed." *Id.* Despite these specific representations, users nevertheless violate the terms and conditions. *Id.* ¶ 14. Violating users are subject to bans but banned users can simply reapply for access to the VDBC. *Id.* ¶ 16. And users get banned only if their activity sufficiently mimics non-human activity; should the bot adapt to OES's anti-scripting algorithm, the bot can evade detection and continue scraping data from the database, albeit more slowly than it otherwise would. *Id.* These experiences demonstrate that OCRA subscriber agreements would be no more effective in policing misuse than subscriber agreements for other OES applications have been.

The current system of access to OCRA, in contrast, keeps PII highly secure at a cost-efficient basis, furthering the "fair and orderly administration of justice." *Courthouse News Serv. v. Schaefer*, 2 F.4th 318, 328 (4th Cir. 2021). Misconduct can be policed effectively because users are asked for their Virginia State Bar number, a unique and easily identifiable number tied to a license to practice law. Dkt. No. 21 ¶ 53. The access and dissemination restrictions imposed in Virginia Code § 17.1-293 are thus narrowly tailored to achieve the Commonwealth's significant government interest of limiting the widespread dissemination of private information more effectively by allowing only lawyers, a self-policing class governed by binding ethics rules that impose significant real world penalties for misuse of data, to view it remotely.

Moreover, OCRA saves significant administrative support and development costs in allowing only officers of the court to use it because the Commonwealth is not required to set up and maintain evolving technical detection methods to identify and ban bots: OCRA accounts tied to a law license prevent a hoard of anonymous bot accounts from crawling the records on OCRA

to harvest the PII in the records. Instead, by relying on "practical obscurity" to prevent bad actors or even lawful profiteers like data brokers from accessing most court records without considerable and repeated expenditure of time and expense, the challenged statute prevents data exploitation.

In all of these ways, the Commonwealth achieves its substantial government interest in the fair, orderly, and efficient administration of justice. Any other system would have to provide a similar vetting process for new users to access the OCRA database. The users would have to be tied to an easily verified real-world identity, there would have to be real-world and significant costs for misusing the data to compensate for the difficulty in apprehending any misuse, and there would have to be some way to ensure that users are truly not looking to harvest and resell the information to data brokers or act as a data broker themselves. *See* **Exhibit A** ¶¶ 13-16. Limiting the class of users to licensed attorneys, their staff (for which the attorney is responsible), clerks, and government agencies meets that standard without imposing a major administrative burden on clerks vetting applicants for a new account. It also limits the number of people applying in the first place, which further reduces the administrative burden on clerks.

Finally, if OCRA's attorney-only access limitation were held to be unconstitutional, absent any further legislative changes, Virginia clerks would still be prohibited from posting PII on the internet under Virginia law. Va. Code § 17.1-293(B). Thus, a clerk could still provide remote access to subscribers, but in order to do so, the clerk would have to redact every court record in their custody containing PII before uploading it to OCRA. Under Virginia law, a clerk is "immune from suit arising from any acts or omissions relating to providing remote access on the Internet pursuant to this section unless the clerk was grossly negligent or engaged in willful misconduct." *Id.* at (G). A clerk cannot simply decline to provide any review and redaction

before publishing court records on the internet without risking losing her immunity from suit for good faith errors caused by records that make it past the review process without complete redaction.

Given that risk, a clerk may determine that given the immense time and fiscal resources needed to be expended on redaction, it would still simply not be worth the clerk's exposure to continue offering OCRA access and cut off the service entirely. Under those circumstances, the "fair and orderly administration of justice," *Schaefer*, 2 F.4th at 328, would be wholly disrupted, leaving many lawyers either unable to perform their duties, or forcing them to expend precious time and resources traveling to courthouses across the state. The end result of this suit could be all parties, including actual litigants and their counsel, sharing the same burdens CNS complains of currently, frustrating the justice system.

IV. OCRA's non-attorney access and dissemination limitations leave open ample alternative channels for communication of the information.

CNS has not pleaded a single instance where Clerk Smith has denied its lawful access to, and dissemination of, courthouse records in Prince William County Circuit Court. Because CNS has an "ample alternative channel" to exercise its rights under the First Amendment in the form of courthouse visitation, the non-attorney and dissemination limitations are constitutional.

The government may impose reasonable restrictions on the time, place, or manner of protected speech, provided "they leave open ample alternative channels for communication of the information." *McCullen v. Coakley*, 134 S. Ct. 2518 (2014) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791). Because the challenged restriction here relates to access of court records, *Nixon vs. Warner Comm'cns, Inc.*, 435 U.S. 589 (1978) is particularly instructive. In that case, broadcasters petitioned for access to tapes admitted into evidence and played at a criminal trial arising out of the "Watergate" scandal. *Id.* at 591-594. Specifically, the

broadcasters sought to copy, broadcast, and sell to the public the portions of the tapes played at trial. *Id.* at 594. The Supreme Court found that, because the public had been able to listen to the tape recordings played in court, they had no right to physical access to the tapes as long as the transcripts were made available. *Id.* at 609.

Here, as in *Nixon*, there is "no question of a truncated flow of information to the public." *Id.* Indeed, CNS has not alleged that its practice of courthouse visitation in Prince William County has resulted in any diminution of newsworthy information to collect. Clerk Smith does not "deny or unwarrantedly abridge the opportunities for the communication of thought." *See Courthouse News Serv. v. Planet*, 947 F.3d 581, 605-06 (2020) (Smith, J., concurring). As stipulated, Clerk Smith provides CNS with access to all non-confidential records, through its public access terminals during normal business hours. Dkt. No. 55 ¶¶ 25-26. No court has found that the First Amendment requires more access than a clerk can provide at the courthouse. Accordingly, because courthouse visitation is an alternative channel for CNS to exercise its First Amendment rights, OCRA's non-attorney access and dissemination limitations do not burden those First Amendment rights.

CONCLUSION

"The First Amendment does not require courts, public entities with limited resources, to set aside their judicial operational needs to satisfy the immediate demands of the press." *Planet*, 947 F.3d at 598. But in this suit, in order to reduce business expenses, CNS asks this Court to set aside a system of remote access by which attorneys receive the PII they need to perform their duties as advocates, and by which the Commonwealth prevents exploitation of litigants' sensitive personal information. These significant government interests would be achieved far less effectively without the challenged limitations, which are narrowly tailored to

achieve those government interests. Accordingly, OCRA's non-attorney access and dissemination limitations pass constitutional muster.

Wherefore, for the foregoing reasons, the Commonwealth respectfully requests that this Court grant its Motion for Summary Judgment, dismiss the claims brought against Defendant Jacqueline C. Smith with prejudice, and award the defendants any further relief that the Court deems necessary and proper.

Respectfully submitted,

COMMONWEALTH OF VIRGINIA

By: */s/ Robert B. McEntee, III*
Counsel

Jason S. Miyares
Attorney General

Steven G. Popps
Deputy Attorney General

Jacqueline C. Hedblom
Senior Assistant Attorney General/
Acting Trial Section Chief

Robert B. McEntee, III (VSB No. 89390)
Erin R. McNeill (VSB No. 78816)
Assistant Attorneys General
Office of the Attorney General
202 North Ninth Street
Richmond, Virginia 23219
(804) 786-8198 – Telephone
(804) 371-2087 – Facsimile
rmcenteeiii@oag.state.va.us
emcneill@oag.state.va.us

CERTIFICATE OF SERVICE

I hereby certify that on July 9, 2022, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to all counsel of record for the parties.

/s/ Robert B. McEntee, III
Robert B. McEntee, III